WE CLAIM

1. A data processing apparatus, comprising:

a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being operable such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode;

a memory operable to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the memory containing a non-secure table and a secure table, the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor, and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor; and

a memory management unit operable, upon receipt of a memory access request issued by the processor when access to an item of data in the memory is required, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory, the memory management unit comprising an internal storage unit operable to store descriptors retrieved by the memory management unit from either the non-secure table or the secure table, and the internal storage unit comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table;

when the processor is operating in said at least one non-secure mode, the memory management unit being operable to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table, and when the processor is operating in said at least one secure mode, the memory management unit being operable to perform the predetermined access control functions for the memory

access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the secure table.

2. A data processing apparatus as claimed in Claim 1, wherein in said at least one non-secure mode the processor is operable under the control of a non-secure operating system, and in said at least one secure mode the processor is operable under the control of a secure operating system, and wherein the descriptors in the non-secure table are generated by the non-secure operating system and the descriptors in the secure table are generated by the secure operating system.

3. A data processing apparatus as claimed in Claim 1, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region.

4. A data processing apparatus as claimed in Claim 3, wherein the internal storage unit comprises a main translation lookaside buffer (TLB) operable to store the descriptors retrieved from the non-secure table or the secure table, and a micro-TLB operable to store as access control information the physical address portions obtained from corresponding descriptors in the main TLB for a number of corresponding virtual address portions, the memory management unit being operable to perform the conversion of the virtual address to the physical address with reference to the content of the micro-TLB.

5. A data processing apparatus as claimed in Claim 4, wherein the micro-TLB is flushed whenever the mode of operation of the processor changes between a secure mode and a non-secure mode, in the secure mode physical address portions only being transferred to the micro-TLB from a descriptor in the main TLB that said associated flag indicates is from the secure table, and in the non-secure mode physical address portions only being transferred to the micro-TLB from a descriptor in the main TLB that said associated flag indicates is from the non-secure table.

6. A data processing apparatus as claimed in Claim 1, wherein the non-secure table comprises a plurality of non-secure tables, each non-secure table containing descriptors pertaining to an associated process executable on the processor, the secure table comprises a plurality of secure tables, each secure table containing descriptors pertaining to an associated process executable on the processor, and the internal storage unit comprises an additional flag associated with each descriptor stored within the internal storage unit to identify the associated process to which that descriptor pertains.

7. A data processing apparatus as claimed in Claim 6, wherein when the memory management unit needs to access the internal storage unit to derive access control information for use in performing the predetermined access control functions, the memory management unit determines from the flag and the additional flag for each descriptor in the internal storage unit whether the internal storage unit contains a descriptor that corresponds to the current mode of operation of the processor and the current process being executed on the processor.

8. A data processing apparatus as claimed in Claim 2, further comprising partition checking logic managed by the secure operating system, and operable whenever the memory access request is issued by the processor when operating in said non-secure mode to detect if the memory access request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request.

9. A data processing apparatus as claimed in Claim 8, wherein the partition checking logic is operable, when the processor is operating in said at least one non-secure mode, to prevent the internal storage unit from storing access control information that would allow access to said secure memory.

10. A data processing apparatus as claimed in Claim 9 wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region, and wherein the partition checking logic is

operable, when the processor is operating in said at least one non-secure mode, to prevent the internal storage unit from storing as access control information the physical address portion if the physical address that would then be produced for the virtual address is within the secure memory.

11. A data processing apparatus as claimed in Claim 9 wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region, wherein the internal storage unit comprises a main translation lookaside buffer (TLB) operable to store the descriptors retrieved from the non-secure table or the secure table, and a micro-TLB operable to store as access control information the physical address portions obtained from corresponding descriptors in the main TLB for a number of corresponding virtual address portions, the memory management unit being operable to perform the conversion of the virtual address to the physical address with reference to the content of the micro-TLB, and wherein the partition checking logic is operable, when the processor is operating in said at least one non-secure mode, to prevent the transfer of a physical address portion from the main TLB to the micro-TLB that would allow access to said secure memory.

12. A data processing apparatus as claimed in Claim 9, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region, and wherein in the event that a descriptor within the non-secure table is associated with a memory region that at least partially incorporates a part of the secure memory, the partition checking logic is operable, when the processor is operating in non-secure mode, to prevent the internal storage unit from storing as access control information the physical address portion specified by that descriptor if the physical address that would then be produced for the virtual address is within the secure memory.

13. A method of managing access to a memory in a data processing apparatus, the data processing apparatus comprising a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being operable such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, the memory being operable to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the memory containing a non-secure table and a secure table, the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor, and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor, the method comprising the steps of:

(i) issuing from the processor a memory access request when access to an item of data in the memory is required;

(ii) determining whether an internal storage of a memory management unit contains a required descriptor from which access control information can be derived to enable the memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request to the memory;

(iii) in the event that the required descriptor is not contained within the internal storage unit, retrieving from either the non-secure table or the secure table, depending on the mode of operation of the processor, the required descriptor, storing that required descriptor within the internal storage unit, and setting a flag to be associated with that required descriptor within the internal storage unit to identify whether that required descriptor is from said non-secure table or said secure table; and

(iv) using the access control information derived from the required descriptor to perform within the memory management unit one or more predetermined access control functions to control issuance of the memory access request to the memory;

such that when the processor is operating in said at least one non-secure mode, the memory management unit performs the predetermined access control functions for

the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table, and when the processor is operating in said at least one secure mode, the memory management unit performs the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the secure table.

14. A method as claimed in Claim 13, wherein in said at least one non-secure mode the processor is operable under the control of a non-secure operating system, and in said at least one secure mode the processor is operable under the control of a secure operating system, and wherein the descriptors in the non-secure table are generated by the non-secure operating system and the descriptors in the secure table are generated by the secure operating system.

15. A method as claimed in Claim 13, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region.

16. A method as claimed in Claim 15, wherein the internal storage unit comprises a main translation lookaside buffer (TLB) for storing the required descriptor retrieved from the non-secure table or the secure table, and a micro-TLB for storing as access control information the physical address portion obtained from the required descriptor in the main TLB, the memory management unit being operable to perform the conversion of the virtual address to the physical address with reference to the content of the micro-TLB.

17. A method as claimed in Claim 16, further comprising the steps of:

flushing the micro-TLB whenever the mode of operation of the processor changes between a secure mode and a non-secure mode;

in the secure mode, only transferring physical address portions to the micro-TLB from a descriptor in the main TLB that said associated flag indicates is from the secure table; and

in the non-secure mode, only transferring physical address portions to the micro-TLB from a descriptor in the main TLB that said associated flag indicates is from the non-secure table.

18. A method as claimed in Claim 13, wherein the non-secure table comprises a plurality of non-secure tables, each non-secure table containing descriptors pertaining to an associated process executable on the processor, the secure table comprises a plurality of secure tables, each secure table containing descriptors pertaining to an associated process executable on the processor, and the internal storage unit comprises an additional flag associated with each descriptor stored within the internal storage unit and settable to identify the associated process to which that descriptor pertains.

19. A method as claimed in Claim 18, wherein when the memory management unit accesses the internal storage unit at said step (ii), the method comprises the step of:

determining from the flag and the additional flag for each descriptor in the internal storage unit whether the internal storage unit contains the required descriptor corresponding to the current mode of operation of the processor and the current process being executed on the processor.

20. A method as claimed in Claim 14, wherein the data processing apparatus further comprises partition checking logic managed by the secure operating system, and operable whenever the memory access request is issued by the processor when operating in said non-secure mode to perform the step of:

detecting if the memory access request is seeking to access the secure memory; and

upon such detection, preventing the access specified by that memory access request.

21. A method as claimed in Claim 20, wherein, when the processor is operating in said at least one non-secure mode, the partition checking logic prevents the internal storage unit from storing access control information that would allow access to said secure memory.

22. A method as claimed in Claim 21, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region, and wherein, when the processor is operating in said at least one non-secure mode, the partition checking logic prevents the internal storage unit from storing as access control information the physical address portion if the physical address that would then be produced for the virtual address is within the secure memory.

23. A method as claimed in Claim 21, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region, wherein the internal storage unit comprises a main translation lookaside buffer (TLB) for storing the required descriptor retrieved from the non-secure table or the secure table, and a micro-TLB for storing as access control information the physical address portion obtained from the required descriptor in the main TLB, the memory management unit being operable to perform the conversion of the virtual address to the physical address with reference to the content of the micro-TLB, and wherein, when the processor is operating in said at least one non-secure mode, the partition checking logic prevents the transfer of a physical address portion from the main TLB to the micro-TLB that would allow access to said secure memory.

24. A method as claimed in Claim 21, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the

corresponding memory region, and wherein in the event that a descriptor within the non-secure table is associated with a memory region that at least partially incorporates a part of the secure memory, the method comprises the step of:

when the processor is operating in non-secure mode, employing the partition checking logic to prevent the internal storage unit from storing as access control information the physical address portion specified by that descriptor if the physical address that would then be produced for the virtual address is within the secure memory.